

---

**Security Review Report**  
**NM-0246 NFT GATED MERKLE DISTRIBUTOR**

---



**NETHERMIND**  
**SECURITY**

(May 23, 2024)

# Contents

<b>1 Executive Summary</b>	<b>2</b>
<b>2 Audited Files</b>	<b>2</b>
<b>3 System Overview</b>	<b>3</b>
3.1 NFTGatedMerkleDistributor .....	3
<b>4 Risk Rating Methodology</b>	<b>4</b>
<b>5 Documentation Evaluation</b>	<b>5</b>
<b>6 Test Suite Evaluation</b>	<b>6</b>
6.1 Contracts Compilation .....	6
6.2 Tests Output .....	6
<b>7 About Nethermind</b>	<b>7</b>

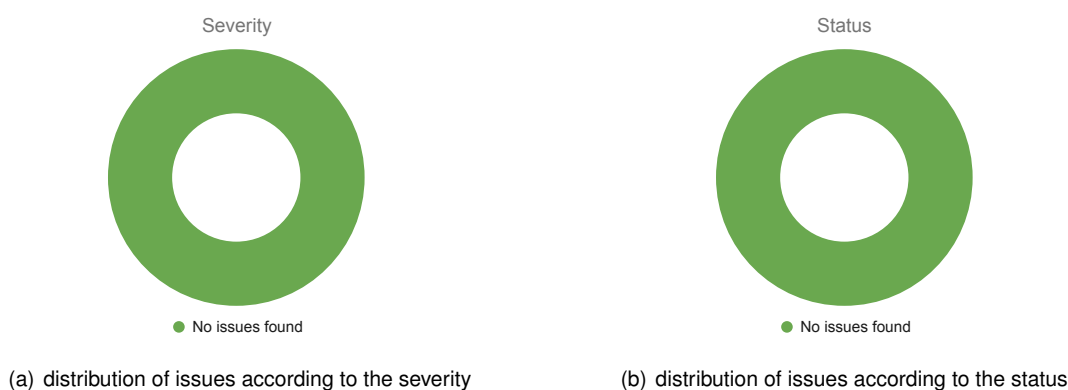
# 1 Executive Summary

This document presents the security review conducted by [Nethermind Security](#) for an extension built for the [MerkleTreeDistributor](#) contract developed by [EthSign](#).

The extension allows the creation of **NFTGatedMerkleTreeDistributor**; this new version of the **MerkleTreeDistributor** effectively tokenizes the claiming rights over the distributed assets. This is achieved by assigning the distribution to a specific token from an NFT collection instead of directly to a user. The token's owner will be the user with the right to claim the token allocation.

The audited code comprises 108 lines of code in Solidity. The EthSign team has provided the necessary explanations to assist the audit. The audit was performed using: (a) manual analysis of the codebase, (b) automated analysis tools, and (c) simulation of the smart contracts. **No issues were found during the duration of the engagement.**

**This document is organized as follows.** Section 2 presents the files in the scope of this audit. Section 3 presents the system overview. Section 4 discusses the risk rating methodology adopted for this audit. Section 5 discusses the documentation provided by the client for this audit. Section 6 presents the compilation, tests, and automated tests. Section 7 concludes the document.



**Fig 1: (a) Distribution of issues: Critical (0), High (0), Medium (0), Low (0), Undetermined (0), Informational (0), Best Practices (0). (b) Distribution of status: Fixed (0), Acknowledged (0), Mitigated (0), Unresolved (0)**

## Summary of the Audit

<b>Audit Type</b>	Security Review
<b>Initial Report</b>	May 23, 2024
<b>Final Report</b>	May 23, 2024
<b>Methods</b>	Manual Review, Automated Analysis
<b>Repository</b>	<a href="#">merkle-token-distributor</a>
<b>Commit Hash</b>	<a href="#">6dc138877a91e7f53a5d00df208419085300c87d</a>
<b>Final Commit Hash</b>	<a href="#">6dc138877a91e7f53a5d00df208419085300c87d</a>
<b>Documentation</b>	Not Available
<b>Documentation Assessment</b>	Medium
<b>Test Suite Assessment</b>	Medium

## 2 Audited Files

	Contract	LoC	Comments	Ratio	Blank	Total
1	<a href="#">src/core/extensions/custom/NFTGatedMerkleDistributor.sol</a>	90	9	10.0%	14	113
2	<a href="#">src/utis/DelegateXYZProvider.sol</a>	18	3	16.7%	3	24
	<b>Total</b>	<b>108</b>	<b>12</b>	<b>11.1%</b>	<b>17</b>	<b>137</b>

### 3 System Overview

EthSign is a hybrid (on-chain and off-chain) implementation of a token management platform that provides advanced tools to streamline the operations involved in securely unlocking and distributing tokens. Fig 2 presents the reviewed contract and its integration with the current system.

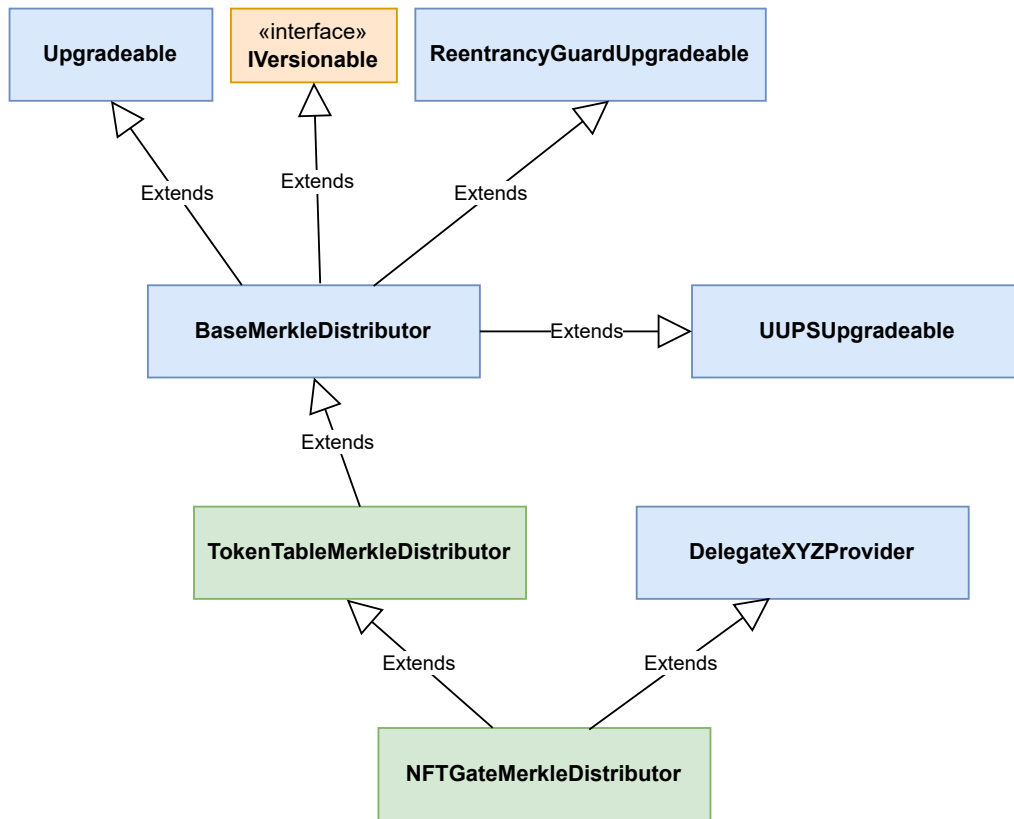


Fig. 2: Structural diagram for the audited contracts

The system implements a solution based on Merkle Tree that converts token unlocking schedules into discrete airdrops off-chain, encodes all airdrops into leaves, generates a Merkle root, and saves it into the `TokenTableMerkleDistributor`. This functionality aims to be applied when there are many recipients. When users attempt to claim, their addresses are checked in the off-chain database to scan for airdrops that belong to them. This process involves cross-referencing with the smart contract to filter out used leaf nodes, indicating that the airdrop has already been claimed.

#### 3.1 NFTGatedMerkleDistributor

The `NFTGatedMerkleDistributor` extends the existing functionality from the `TokenTableMerkleDistributor` contract. It adds one more variable to the contract’s state; the variable is named `nft`, and it is part of the following struct.

```

1 struct NFTGatedMerkleDistributorStorage {
2     address nft;
3 }
    
```

The data used for describing a specific allocation is also extended with two new fields: `expiryTimestamp` and `nftTokenId`.

```

1 struct NFTGatedMerkleDistributorData {
2     TokenTableMerkleDistributorData base;
3     uint256 expiryTimestamp; // The airdrop can't be claimed past this timestamp. 0 == no expiry.
4     uint256 nftTokenId; // Used to infer the eligible claimer (aka current owner or an address authorized by owner
5     // through delegate.xyz)
6 }
    
```

The `expiryTimestamp` adds a new feature to claims. It now allows to make claims that are only valid during certain periods. Users can only claim a specific allocation if the current timestamp exceeds `expiryTimestamp`.

The **nftTokenId** is used to tokenize the claiming rights of the allocation. Previously, allocations were assigned to users and could not be changed. With the approach introduced by this extension, allocations are assigned to a specific NFT token, and the token's owner is the user with the right to claim the allocation. If a user decides to transfer the NFT with the allocation assigned, they would also be transferring the right to claim.

The **NFTGatedMerkleDistributor** also introduces the use of **DelegateXYZ**. DeDelegateXYZ is a solution to secure valuable on-chain assets while still participating in NFT airdrop claims, ERC20 token governance, and more. Users link cold wallets with hot wallets, and then the hot wallet can act on behalf of the cold wallet, like crypto power-of-attorney. Users can use this feature to delegate the right to claim to another account without transferring their NFT. It is important to note that delegations are linked to the token's owner, so if the token is transferred, past delegations are not longer valid.

The **NFTGatedMerkleDistributor** adds a few other changes: no fees are charged while claiming the allocations, and the previous implementation of the delegate feature is disabled.

## 4 Risk Rating Methodology

The risk rating methodology used by **Nethermind Security** follows the principles established by the **OWASP Foundation**. The severity of each finding is determined by two factors: **Likelihood** and **Impact**.

**Likelihood** measures how likely an attacker will uncover and exploit the finding. This factor will be one of the following values:

- a) **High**: The issue is trivial to exploit and has no specific conditions that need to be met;
- b) **Medium**: The issue is moderately complex and may have some conditions that need to be met;
- c) **Low**: The issue is very complex and requires very specific conditions to be met.

Other factors are also considered when defining the likelihood of a finding. These can include but are not limited to Motive, opportunity, exploit accessibility, ease of discovery, and ease of exploit.

**Impact** is a measure of the damage that may be caused if an attacker exploits the finding. This factor will be one of the following values:

- a) **High**: The issue can cause significant damage, such as loss of funds or the protocol entering an unrecoverable state;
- b) **Medium**: The issue can cause moderate damage, such as impacts that only affect a small group of users or only a particular part of the protocol;
- c) **Low**: The issue can cause little to no damage, such as bugs that are easily recoverable or cause unexpected interactions that cause minor inconveniences.

Other factors are also considered when defining the impact of a finding. These can include but are not limited to Data/state integrity, loss of availability, financial loss, and reputation damage. After defining the likelihood and impact of an issue, the severity can be determined according to the table below.

		Severity Risk		
		Medium	High	Critical
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Info/Best Practices	Low	Medium
	Undetermined	Undetermined	Undetermined	Undetermined
		Low	Medium	High
		Likelihood		

To address issues that do not fit a High/Medium/Low severity, **Nethermind Security** also uses three more finding severities: **Informational**, **Best Practices**, and **Undetermined**.

- a) **Informational** findings do not pose any risk to the application, but they carry some information that the audit team intends to pass to the client formally;
- b) **Best Practice** findings are used when some piece of code does not conform with smart contract development best practices;
- c) **Undetermined** findings are used when we cannot predict the impact or likelihood of the issue.

## 5 Documentation Evaluation

Software documentation refers to the written or visual information describing software's functionality, architecture, design, and implementation. It provides a comprehensive overview of the software system and helps users, developers, and stakeholders understand how the software works, how to use it, and how to maintain it. Software documentation can take different forms, such as user manuals, system manuals, technical specifications, requirements documents, design documents, and code comments. Software documentation is critical in software development, enabling effective communication between developers, testers, users, and other stakeholders. It helps to ensure that everyone involved in the development process has a shared understanding of the software system and its functionality. Moreover, software documentation can improve software maintenance by providing a clear and complete understanding of the software system, making it easier for developers to maintain, modify, and update the software over time. Smart contracts can use various types of software documentation. Some of the most common types include:

- Technical whitepaper: A technical whitepaper is a comprehensive document describing the smart contract's design and technical details. It includes information about the purpose of the contract, its architecture, its components, and how they interact with each other;
- User manual: A user manual is a document that provides information about how to use the smart contract. It includes step-by-step instructions on how to perform various tasks and explains the different features and functionalities of the contract;
- Code documentation: Code documentation is a document that provides details about the code of the smart contract. It includes information about the functions, variables, and classes used in the code, as well as explanations of how they work;
- API documentation: API documentation is a document that provides information about the API (Application Programming Interface) of the smart contract. It includes details about the methods, parameters, and responses that can be used to interact with the contract;
- Testing documentation: Testing documentation is a document that provides information about how the smart contract was tested. It includes details about the test cases that were used, the results of the tests, and any issues that were identified during testing;
- Audit documentation: Audit documentation includes reports, notes, and other materials related to the security audit of the smart contract. This type of documentation is critical in ensuring that the smart contract is secure and free from vulnerabilities.

These types of documentation are essential for smart contract development and maintenance. They help ensure that the contract is properly designed, implemented, and tested, and they provide a reference for developers who need to modify or maintain the contract in the future.

### Remarks about EthSign documentation

No documentation has been provided besides NatSpec comments in the contract. However, the EthSign team was available to address any inquiries or concerns raised by the Nethermind Security team and explained all the introduced features to our team.

## 6 Test Suite Evaluation

### 6.1 Contracts Compilation

```
forge build
[] Compiling...
[] Compiling 81 files with 0.8.24
[] Solc 0.8.24 finished in 7.91s
Compiler run successful!
```

### 6.2 Tests Output

```
Ran 16 tests for test/TokenTableMerkleDistributor.t.sol:TokenTableMerkleDistributorTest
[PASS] testFuzz_claim_fail_notActive(uint128,uint128)
[PASS] testFuzz_decodeLeaf(uint256,uint256,uint256)
[PASS] testFuzz_delegateClaim_fail_notActive(address,uint128,uint128)
[PASS] testFuzz_delegateClaim_fail_notDelegate(address,uint128,uint128)
[PASS] testFuzz_encodeLeaf_verify_and_claim(address[],bytes32[],uint256[],uint64[],uint128[])
[PASS] testFuzz_encodeLeaf_verify_and_delegateClaim(address,address[],bytes32[],uint256[],uint64[],uint128[])
[PASS] testFuzz_encodeLeaf_verify_no_claim(address[],bytes32[],uint256[],uint256[],uint256[])
[PASS] testFuzz_externalTTUFeeCollector_erc20Fees(address[],bytes32[],uint256[],uint64[],uint128[])
[PASS] testFuzz_externalTTUFeeCollector_etherFees(address[],bytes32[],uint256[],uint64[],uint128[])
[PASS] testFuzz_setBaseParams_fail_badTime(address,uint256,uint256,bytes32)
[PASS] testFuzz_setBaseParams_fail_notOwner(address,address,uint256,uint256,bytes32)
[PASS] testFuzz_setBaseParams_succeed_0(address,uint256,uint256,bytes32)
[PASS] testFuzz_setClaimDelegate_fail_notOwner(address,address)
[PASS] testFuzz_setClaimDelegate_succeed_0(address)
[PASS] testFuzz_withdraw_fail_notOwner(address)
[PASS] testFuzz_withdraw_succeed_0(uint256)
Suite result: ok. 16 passed; 0 failed; 0 skipped; finished in 43.24s (182.97s CPU time)

Ran 1 test suite in 43.33s (43.24s CPU time): 16 tests passed, 0 failed, 0 skipped (16 total tests)
```

## 7 About Nethermind

Nethermind is a Blockchain Research and Software Engineering company. Our work touches every part of the web3 ecosystem - from layer 1 and layer 2 engineering, cryptography research, and security to application-layer protocol development. We offer strategic support to our institutional and enterprise partners across the blockchain, digital assets, and DeFi sectors, guiding them through all stages of the research and development process, from initial concepts to successful implementation.

We offer security audits of projects built on EVM-compatible chains and Starknet. We are active builders of the Starknet ecosystem, delivering a node implementation, a block explorer, a Solidity-to-Cairo transpiler, and formal verification tooling. Nethermind also provides strategic support to our institutional and enterprise partners in blockchain, digital assets, and decentralized finance (DeFi). In the next paragraphs, we introduce the company in more detail.

**Blockchain Security:** At Nethermind, we believe security is vital to the health and longevity of the entire Web3 ecosystem. We provide security services related to Smart Contract Audits, Formal Verification, and Real-Time Monitoring. Our Security Team comprises blockchain security experts in each field, often collaborating to produce comprehensive and robust security solutions. The team has a strong academic background, can apply state-of-the-art techniques, and is experienced in analyzing cutting-edge Solidity and Cairo smart contracts, such as ArgentX and StarkGate (the bridge connecting Ethereum and StarkNet). Most team members hold a Ph.D. degree and actively participate in the research community, accounting for 240+ articles published and 1,450+ citations in Google Scholar. The security team adopts customer-oriented and interactive processes where clients are involved in all stages of the work.

**Blockchain Core Development:** Our core engineering team, consisting of over 20 developers, maintains, improves, and upgrades our flagship product - the Nethermind Ethereum Execution Client. The client has been successfully operating for several years, supporting both the Ethereum Mainnet and its testnets, and now accounts for nearly a quarter of all synced Mainnet nodes. Our unwavering commitment to Ethereum's growth and stability extends to sidechains and layer 2 solutions. Notably, we were the sole execution layer client to facilitate Gnosis Chain's Merge, transitioning from Aura to Proof of Stake (PoS), and we are actively developing a full-node client to bolster Starknet's decentralization efforts. Our core team equips partners with tools for seamless node set-up, using generated docker-compose scripts tailored to their chosen execution client and preferred configurations for various network types.

**DevOps and Infrastructure Management:** Our infrastructure team ensures our partners' systems operate securely, reliably, and efficiently. We provide infrastructure design, deployment, monitoring, maintenance, and troubleshooting support, allowing you to focus on your core business operations. Boasting extensive expertise in Blockchain as a Service, private blockchain implementations, and node management, our infrastructure and DevOps engineers are proficient with major cloud solution providers and can host applications in-house or on clients' premises. Our global in-house SRE teams offer 24/7 monitoring and alerts for both infrastructure and application levels. We manage over 5,000 public and private validators and maintain nodes on major public blockchains such as Polygon, Gnosis, Solana, Cosmos, Near, Avalanche, Polkadot, Aptos, and StarkWare L2. Sedge is an open-source tool developed by our infrastructure experts, designed to simplify the complex process of setting up a proof-of-stake (PoS) network or chain validator. Sedge generates docker-compose scripts for the entire validator set-up based on the chosen client, making the process easier and quicker while following best practices to avoid downtime and being slashed.

**Cryptography Research:** At Nethermind, our Cryptography Research team is dedicated to continuous internal research while fostering close collaboration with external partners. The team has expertise across a wide range of domains, including cryptography protocols, consensus design, decentralized identity, verifiable credentials, Sybil resistance, oracles, and credentials, distributed validator technology (DVT), and Zero-knowledge proofs. This diverse skill set, combined with strong collaboration between our engineering teams, enables us to deliver cutting-edge solutions to our partners and clients.

**Smart Contract Development & DeFi Research:** Our smart contract development and DeFi research team comprises 40+ world-class engineers who collaborate closely with partners to identify needs and work on value-adding projects. The team specializes in Solidity and Cairo development, architecture design, and DeFi solutions, including DEXs, AMMs, structured products, derivatives, and money market protocols, as well as ERC20, 721, and 1155 token design. Our research and data analytics focuses on three key areas: technical due diligence, market research, and DeFi research. Utilizing a data-driven approach, we offer in-depth insights and outlooks on various industry themes.

**Our suite of L2 tooling:** Warp is Starknet's approach to EVM compatibility. It allows developers to take their Solidity smart contracts and transpile them to Cairo, Starknet's smart contract language. In the short time since its inception, the project has accomplished many achievements, including successfully transpiling Uniswap v3 onto Starknet using Warp.

- **Voyager** is a user-friendly Starknet block explorer that offers comprehensive insights into the Starknet network. With its intuitive interface and powerful features, Voyager allows users to easily search for and examine transactions, addresses, and contract details. As an essential tool for navigating the Starknet ecosystem, Voyager is the go-to solution for users seeking in-depth information and analysis;
- **Horus** is an open-source formal verification tool for StarkNet smart contracts. It simplifies the process of formally verifying Starknet smart contracts, allowing developers to express various assertions about the behavior of their code using a simple assertion language;
- **Juno** is a full-node client implementation for Starknet, drawing on the expertise gained from developing the Nethermind Client. Written in Golang and open-sourced from the outset, Juno verifies the validity of the data received from Starknet by comparing it to proofs retrieved from Ethereum, thus maintaining the integrity and security of the entire ecosystem.

Learn more about us at [nethermind.io](https://nethermind.io).



### General Advisory to Clients

As auditors, we recommend that any changes or updates made to the audited codebase undergo a re-audit or security review to address potential vulnerabilities or risks introduced by the modifications. By conducting a re-audit or security review of the modified codebase, you can significantly enhance the overall security of your system and reduce the likelihood of exploitation. However, we do not possess the authority or right to impose obligations or restrictions on our clients regarding codebase updates, modifications, or subsequent audits. Accordingly, the decision to seek a re-audit or security review lies solely with you.

### Disclaimer

This report is based on the scope of materials and documentation provided by you to [Nethermind](#) in order that [Nethermind](#) could conduct the security review outlined in **1. Executive Summary** and **2. Audited Files**. The results set out in this report may not be complete nor inclusive of all vulnerabilities. [Nethermind](#) has provided the review and this report on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Blockchain technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. This report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on this report in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, [Nethermind](#) disclaims any liability in connection with this report, its content, and any related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. [Nethermind](#) does not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and [Nethermind](#) will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate. FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.